



AF/
27W

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:

APPLICANTS: Riordan
SERIAL NO.: 10/058,661 FILING DATE: 01/28/2002
EXAMINER: Cervetti ART UNIT: 2136
ATTORNEY'S DOCKET NO.: CH9-2000-0011US1
TITLE: EMBEDDED CRYPTOGRAPHIC SYSTEM

Mail Stop Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313

APPELLANT'S BRIEF ON APPEAL

This is an appeal from the Final Office Action dated January 24, 2006, finally rejecting claims 1-13. A Notice of Appeal was filed on May 24, 2006, along with a Request for a Pre-Appeal Brief Conference. A Notice of Panel Decision from Pre-Appeal Brief Review was mailed July 7, 2006, indicating that Applicant should proceed to the Board of Appeals and Interferences. As this Appeal Brief is herewith filed within one month of the decision by the Pre-Appeal Brief Conference panel, no extension of time fee is believed to be due. Please charge deposit account no.: 50-0510 in the amount of \$ 500 for the filing of this appeal brief. If there are any deficiencies in payment, please charge deposit account no.: 50-0510 for any deficiency.

08/10/2006 TBESHAH1 00000025 500510 10058661
01 FC:1402 500.00 DA

TABLE OF CONTENTS

Real Party in Interest	3
Related Appeals and Interferences	4
Status of Claims	5
Status of Amendments After Final	6
Summary of Invention and Claimed Subject Matter	7
Issues	9
Arguments	10
Conclusion	26
Claims Appendix	27
Evidence Appendix	31
Related Proceedings Appendix	32

(1) REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation, of Armonk, New York.

(2) RELATED APPEALS AND INTERFERENCES

The undersigned attorney is not aware of any related appeals or interferences.

(3) STATUS OF CLAIMS

The rejection of claims 1-13 is being appealed.

The status of the claims is as follows:

Claims allowed: none

Claims objected to: none

Claims rejected: Claims 1-13.

Claims canceled: none

(4) STATUS OF AMENDMENTS AFTER FINAL

An amendment after final was proffered to the Patent Office on April 03, 2006. In the Advisory Action dated April 28, 2006, the Patent Office checked off box 7 b) which states "For the purposes of appeal the proposed remarks will be entered and an explanation of how the new claims would be rejected is provided below or appended:" Also, box 11 was checked and claims 1-13 were deemed by the Patent Office to be rejected.

**(5) SUMMARY OF INVENTION AND CLAIMED SUBJECT
MATTER**

This invention concerns plaintext, ciphertext test pairs and is directed to a method for detecting compromise of cryptographic operations because the ciphertext generated by a first cryptographic algorithm from a test plaintext indicates that an apoptosis key has been used (page 4, lines 3-5 and 24-27). Upon detection of an apoptosis key by the generation of ciphertext corresponding to that apoptosis key encrypting the designated plaintext, cryptographic algorithms should be switched (page 4, lines 27-35). An advantage of the solution of this invention is “that there is no need for controlling respectively trusting the manufacturer or a security service” (page 5, lines 11-12).

Claim 1 recites a cryptographic system (1) comprising first cryptographic algorithm means (2) for enabling cryptographic operations, input/output means (3, 4) for receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations, at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i , receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i , checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i , switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6) (page 7, line 16, through page 8, line 1) (“the expression “means” stands for hardware, software, or a combination of hardware and software” – page 9, lines 1-2).

Claim 2 recites “System as claimed in claim 1, wherein said cryptographic system (1) includes at least one second cryptographic algorithm means (8) wherein said switching means (7) enables switching to said at least one second cryptographic algorithm means (8).”

Claim 3 recites “System as claimed in claim 1, wherein said receiving means (5) is made for accepting control streams which include at least one plaintext P_i , for each plaintext P_i a corresponding ciphertext C_i and a corresponding apoptosis key K_i and said checking means (6) is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i .”

Claim 11 recites “A computer software product for operating a cryptographic system (1) for carrying out cryptographic operations, said product is characterized by a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, enable the computer to perform a first cryptographic algorithm that is enabling said cryptographic operations, receive input streams and send output streams wherein said input streams are transformed to said output streams by said cryptographic operations, receive a control stream which is including at least one apoptosis key K_i , check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i , stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i .” (page 7, line 16, through page 8, line 1)

Claim 12 recites “Computer software product as claimed in claim 11, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to one of a plurality of second cryptographic algorithms for said cryptographic operations after said stopping.” (page 8, lines 3-12)

(6) ISSUES

- I. Whether the Patent Office properly rejected claims 1, 3, 5, 7, 8, 10, 11, and 13 under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US Patent Number 6,327,661) and further in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services)?
- II. Whether the Patent Office properly took Official Notice for claim 7 and whether Chorley, U.S. Patent No. 4,634,807, provides an appropriate teaching?
- III. Whether the Patent Office properly rejected claims 2, 4, 6, 9, and 12 under 35 U.S.C. 103(a) as being unpatentable over Kocher and Tschudin, and further in view of Esserman et al., U.S. Patent No. 5,144,664?

(7) ARGUMENT

Issue I

Did the Patent Office properly reject claims 1, 3, 5, 7, 8, 10, 11, and 13 as unpatentable under 35 U.S.C. 103(a) over Kocher et al. (US Patent Number 6,327,661) and further in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services).

It appears that the Patent Office had reiterated verbatim the prior Office Action's prior art rejections in the Final Office Action dated January 24, 2006. The only new arguments by the Patent Office responsive to Applicant's arguments in the response dated November 4, 2005, presented by the Patent Office, appears to be in paragraphs 9-15, of which paragraphs 9-11 appear to be general statements that Applicant addressed on pages 15-16 of the response after final mailed April 3, 2006. Please note Applicant wishes to emphasize that there is no admission as to a limitation on the differences between the prior art and the claimed invention.

The Patent Office rejected claims 1, 3, 5, 7, 8, 10, 11, and 13 under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US Patent Number 6,327,661) and further in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services).

The Patent Office asserted (page 4-5 of the Final Office Action mailed January 24, 2006) "Regarding claim 1, Kocher teaches a cryptographic system comprising first cryptographic algorithm means for enabling cryptographic operations (column 2, lines 60-67, column 13, lines 20-67), input/output means for receiving input streams and sending output streams (column 13, lines 20-67, column 14, lines 61-67), wherein said input streams are transformed to said output streams by said cryptographic operations (column 13, lines 20-67), at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i (column 13, lines 20-67), receiving means for receiving a control stream (column 13, lines 20-67, column 14, lines 1-60), checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first

cryptographic algorithm means (column 13, lines 20-67), switching means for stopping said cryptographic operations with said first cryptographic algorithm means (column 13, lines 20-67), wherein said stopping by said switching means is triggered by said checking means (column 13, lines 20-67). Kocher does not expressly disclose including at least one apoptosis key K_i . Kocher teaches self-destructing keys. However, Tschudin teaches the concept of “apoptosis” related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an “apoptosis key”. One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Kocher (column 2, lines 60-67) discloses “...The following sections describe various embodiments of a general technique of using unpredictable information to protect cryptographic systems (cryptosystems) against external monitoring attacks...”

Kocher (column 13, lines 20-67) discloses “Cryptographic operations should normally be checked to ensure that incorrect computations do not compromise keys or enable other attacks. Cryptographic implementations of the present invention can be, and in a preferred embodiment are, combined with error-detection and/or error-correction logic to ensure that cryptographic operations are performed correctly. For example, a simple and effective technique is to perform cryptographic operations twice, ideally using two independent hardware processors and/or software implementations, with a comparison operation performed at the end to verify that both produce identical results. If the results produced by the two units do not match, the failed comparison will prevent the defective processing result from being used. In situations where security is more important than reliability, if the compare operation ever fails (or fails too many times) the device may self-destruct (such as by deleting internal keys) or disable itself. For example, a device might erase its key storage memory if either two defective DES operations occur sequentially or five defective DES results occur during the lifetime of the device. In some cryptosystems, full redundancy is not necessary. For example, with RSA, methods are known in the background art for self-checking functions that can be incorporated into the cryptosystem implementation (e.g., RSA signatures can be verified after digital signing

operations). Detection of conditions likely to cause incorrect results may also be used. In particular, active or passive sensors to detect unusually high or low voltages, high-frequency noise on voltage or signal inputs, exposure to electromagnetic fields and radiation, and physical tampering may be employed. Inappropriate operating conditions can (for example) trigger the device to reset, delete secrets, or self-destruct. Self-diagnostic functions such as a POST (power-on-self-test) should also be incorporated to verify that cryptographic functions have not been damaged. In cases where an ATR (answer-to-reset) must be provided before a comprehensive self-test can be completed, the self-test can be deferred until after completion of the first transaction or until a sufficient idle period is encountered. For example, a flag indicating successful POST completion can be cleared upon initialization. While the card is waiting for a command from the host system, it can attempt the POST. Any I/O received during the POST will cause an interrupt, which will cancel the POST (leaving the POST-completed flag at zero). If any cryptographic function is called, the device will check the POST flag and (if it is not set) perform the POST before doing any cryptographic operations.”

Kocher (column 14, lines 61-67) discloses “A cryptographic processing device for securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret by external monitoring, comprising: (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) a source of unpredictable information; (c) a processor: (i) connected to said input interface for receiving and cryptographically processing said quantity, (ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by modifying said sequence; and (d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.”

Kocher discloses (column 14, lines 1-60) “The present invention is extremely useful for improving security, particularly in environments and applications with difficult engineering requirements, by enabling the construction of devices that are significantly more resistant to attack than devices of similar cost and complexity that do not use the

present invention. Also, multiple security techniques may be required to make a system secure. For example, leak minimization and obfuscation may be used in conjunction with other security methods or countermeasures. As those skilled in the art will appreciate, the techniques described above are not limited to particular host environments or form factors...”

Kocher does not disclose or fairly suggest “ciphertext,” “test plaintext,” “test ciphertext,” “an apoptosis key,” “a control stream,” “checking means,” “receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,” “switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6),” nor “checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i ”.

The Patent Office, with reference to independent claims 5 and 11, asserted that column 2, lines 60-67 and column 3, lines 1-10, provide a teaching for the limitation of “implementing within said cryptographic system a first cryptographic algorithm enabling said cryptographic operations” (claim 5) and “which instructions, when read by a computer, enable the computer to perform a first cryptographic algorithm that is enabling said cryptographic operations” (claim 11).

Kocher discloses (column 2, line 60, through column 3, line 10) “The following sections describe various embodiments of a general technique of using unpredictable information to protect cryptographic systems (cryptosystems) against external monitoring attacks...”

The cited passage of Kocher (column 2, line 60, through column 3, line 10) does not appear to disclose a first cryptographic algorithm.

The Patent Office asserted that Kocher discloses “checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding

test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (column 13, lines 20-67).”

Specifically, claim 1 recites “checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i , switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6).”

Claim 5 recites “selecting at least one test plaintext P_i and enciphering each test plaintext P_i with said first cryptographic algorithm and with a corresponding apoptosis key K_i thereby generating a corresponding test ciphertext C_i for each test plaintext P_i , implementing within said cryptographic system (1) said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i , implementing within said cryptographic system (1) receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i , implementing within said cryptographic system (1) checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i , implementing within said cryptographic system (1) switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm, wherein said stopping by said switching means (7) is triggered by said checking means (6).

Claim 8 recites “checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i , stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i .”

Claim 11 recites “check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i , stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i .”

In the claimed invention, if the test ciphertext corresponds to the test plaintext that results from the apoptosis key, the first cryptographic algorithm is stopped.

Kocher does not disclose checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i . Furthermore, Kocher does not disclose test plaintext, test ciphertext pairs. Instead, Kocher (col. 13, lines 20-67) discloses cryptographic operations should normally be checked to ensure that incorrect computations do not compromise keys or enable other attacks. Kocher discloses a technique of performing cryptographic operations twice, ideally using two independent processors and/or software implementations, with a comparison operation performed at the end to verify that both produce identical results. Kocher discloses, in situations where security is more important than reliability, the device may disable itself or self-destruct (e.g., by deleting internal keys) if the comparison of two cryptographic operations fails. In contrast, applicant discloses the stopping of a first cryptographic algorithm if a test ciphertext is generated for a test plaintext that corresponds to an apoptosis key. Kocher does not disclose or suggest the checking using a test plaintext, a test ciphertext, and an apoptosis key, as has been claimed.

Tschudin discloses a need for a self-destruction mechanism inside a distributed mobile service (abstract). Tschudin discloses the execution of a self-destruction routine that depends on “environmental data” as requested by a read() instruction and provides an example of apoptosis in response to the decryption, via a key, of code encrypted at an originator’s site (section 3.1) and then processed at the executing site. Tschudin does not

disclose or suggest the checking using a test plaintext, a test ciphertext, and an apoptosis key, as has been claimed.

Although Kocher and Tschudin are both concerned with cryptographic techniques, their disclosed approaches are starkly different. Kocher checks internally for security compromises in a smartcard environment (e.g., checking for discrepancies between two test results) while Tschudin is vigilant for a kill message to arrive from an external source in a distributed mobile service environment. Kocher discloses multiple cryptographic operations using encryptors that yield results that are later compared whereas Tschudin checks for and decrypts an encrypted kill message that leads to termination of distributed services. Kocher also does not disclose a decryptor that has been relied upon by Tschudin to check for an apoptosis message. Accordingly, Kocher does not readily lend itself to modification by Tschudin.

Neither Kocher nor Tschudin, alone or in combination, disclose or fairly suggest “a control stream,” “checking means,” “receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,” nor “checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i ”.

The Patent Office asserted (page 5, lines 3-9 of the Final Office Action mailed January 24, 2006) “Kocher et al. do not expressly disclose including at least one apoptosis key K_i . Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of “apoptosis” related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an “apoptosis key”. One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).”

In the Advisory Action dated April 28, 2006, the Patent Office asserted

Furthermore, Tschudin expressly teach using a received key for decryption and looking at the result (test) to decide if it was a valid decryption or not (page 258), clearly contradicting Applicant's assertion that Kocher or Tschudin do not disclose or suggest "ciphertext," "test plaintext," "apoptosis key," etc. The decryption performed by Tschudin (page 258) clearly provides the teaching of using a key (apoptosis or not) and based on the result determining whether the decryption is valid or not. Tschudin clearly teaches checking using test values (page 258), namely "for each presented key we attempt to decrypt the ENCRYPTED_CODE. Looking at the result we can decide if this was a valid decryption or not.

Tschudin was discussed in the originally filed specification, page 2, line 27, through page 3, line 8 as follows:

In the field of rather complex systems a concept for secure shutting down of mobile services is described by Christian Tschudin "Apoptosis the Programmed Death of Distributed Services", in J. Vitek and C. Jensen, editors, Secure Internet Programming--Security Issues for Mobile and Distributed Objects, pages 253-260, Springer, 1999. Active networks with services run by mobile code have to have the functionality of creating and ending services. The apoptosis concept of self-destructing mobile services is borrowed from cell biology and designates there the programmed cell death. The apoptosis process is suggested to start as for cells by two different ways. A service may depend on a continuous stream of credentials or positive signals. Once these credentials run out, the service will shut down. According to the second way a negative signal causes the service to shut down.

The apoptosis entry point of a mobile service would be a primary target for an attack. Therefore the apoptosis concept should be implemented with cryptographic security functions. Cryptographic security functions are described by J. Riordan and B. Schneier, Environmental Key Generation Towards Clueless Agents, in G. Vigna,

editor, Mobile Agents and Security, volume 1419 of LNCS, pages 15-24, Springer, 1998. The shut down could be induced by an apoptosis activator. **Applying the above-mentioned apoptosis concept does not change the disadvantage that a system administrator or a security service provider has to induce the shut down procedure.**

In the Advisory Action dated May 5, 2006, the Patent Office asserted

An apoptosis key, as disclosed, is nothing more than a key that has been changed (dead, expired, not in use, etc.). Thus, it would have been obvious to someone of ordinary skill in the art to check if an expired key is being used. Checking whether an expired key has been used to attempt access to a computer system is conventional and well known. Authentication methods for computer systems prompting users to change a password (key) after a certain amount of time had passed, were conventional and well known at the time the invention was made. It was also conventional and well known to prevent the re-use of a certain key by a certain user. This necessarily implies that an old key was saved to verify the user did not attempt to use the same key at a later time.

During patent examination, the pending claims must be "given *>their<* broadest reasonable interpretation **consistent with the specification.**" *>In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000). MPEP 2111. Whereas the Patent Office has tried to define the apoptosis key of the applicant as "a key that has been changed"; i.e., "dead, expired, not in use, etc.;" a reading of Applicant's disclosure indicates that Applicant is concerned with keys that have been compromised in cases where the cryptographic algorithm has been broken (e.g., page 4, lines 15-30; page 8, lines 14-29).

Neither Kocher nor Tschudin disclose or suggest the claimed technique which determines the existence of an apoptosis key, considered a compromise situation, when a test plaintext generates a corresponding test ciphertext under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i .

Thus, claims 1-13 are not made obvious by Kocher and Tschudin, either alone or in combination.

Claims 8 and 11

Claim 8

Claim 8 is patentably distinct from claims 1, 5, and 11 because claim 8 relates to a method for operating a cryptographic system for carrying out cryptographic operations whereas claim 1 relates to a cryptographic system, claim 5 relates to a method for creating a cryptographic system, and claim 11 relates to a computer software product for operating a cryptographic system for carrying out cryptographic operations.

Claim 11

Claim 11 is patentably distinct from claims 1, 5, and 11 because claim 11 relates to a computer software product for operating a cryptographic system for carrying out cryptographic operations whereas claim 1 relates to a cryptographic system, claim 5 relates to a method for creating a cryptographic system, and claim 8 relates to relates to a method for operating a cryptographic system for carrying out cryptographic operations.

Claim 1 and 5

Claims 1 and 5 further recite **“switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6).”**

Neither Kocher nor Tschudin disclose or fairly suggest **“switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6).”** Thus, claims 1 and 5 are allowable over the prior art of record.

Claim 1

Claim 1 is patentably distinct from claim 5 as claim 1 relates to a cryptographic system and claim 5 relates to a method for creating a cryptographic system for carrying out cryptographic operations.

Claim 5

Claim 5 is patentably distinct from claim 1 as claim 1 relates to a cryptographic system and claim 5 relates to a method for creating a cryptographic system for carrying out cryptographic operations.

Claim 3

Claim 3 recites “System as claimed in claim 1, wherein said receiving means (5) is made for accepting control streams which include at least one plaintext P_i , for each plaintext P_i a corresponding ciphertext C_i and a corresponding apoptosis key K_i and said checking means (6) is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i .”

The Patent Office asserted (page 5, lines 10-18, of the Final Office Action mailed January 24, 2006) “Regarding claim 3, the combination of Kocher and Tschudin teaches the limitations as set forth under claim 1 above. Furthermore, Kocher teaches said receiving means is made for accepting control streams which includes at least one plaintext P_i , for each plaintext P_i a corresponding ciphertext C_i (column 2, lines 60-67, column 3, lines 1-10) and said checking means is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i (column 13, lines 20-67, column 14, lines 61-67) and Tschudin teaches the concept of “apoptosis” related to distributed services and computer security (sections 3-5).”

Claim 10

Claim 10 recites “Method as claimed in claim 8, wherein said receiving of a control stream includes for each apoptosis key K_i receiving of a plaintext P_i and a corresponding ciphertext C_i , and said checking includes trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , and said received ciphertext C_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i .”

Neither Kocher nor Tschudin appear to disclose or fairly suggest “said checking includes trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , and said received ciphertext C_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i .”

Thus, claim 10 is allowable over the prior art of record. Claim 10 is patentably distinct from claim 8 because claim 10 further limits claim 8 with subject matter that is new and not obvious.

Claim 13

Claim 13 recites “Computer program comprising program code means for performing the steps of claim 8 when said program is run on a computer.”

Claim 13 is patentably distinct from claim 8 because claim 8 relates to a method for operating a cryptographic system and claim 13 relates to a computer program comprising program code. Claim 13 is allowable because it depends from claim 8.

Issue II

Did the Patent Office properly take Official Notice for claim 7 and does Chorley, U.S. Patent No. 4,634,807, provide an appropriate teaching and is it combinable with Kocher and Tschudin?

Claim 7

The Patent Office asserted (page 6, last two lines, through page 7, line 6, of the Final Office Action mailed January 24, 2006) “Regarding claim 7, the combination of

Kocher et al. and Tschudin does not expressly disclose publishing said at least one test plaintext P_i and for each test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i . However, Examiner takes Official Notice that publishing information was conventional and well known at the time the invention was made. Furthermore, Kocher et al. stores plaintext and ciphertext prior to comparing them. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish this information since Examiner takes Official Notice that it was conventional and well known.”

Applicant had challenged the Patent Office on the taking of Official Notice and had requested a teaching applicable to Kocher and Tschudin (or other asserted reference or combination of references) that allegedly discloses or makes obvious claim 7 including limitations from base claim 5 and specifically requests a teaching for the limitation of “the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i .”

The Patent Office asserted (page 4, lines 3-6, of the Final Office Action mailed January 24, 2006) “In response to Applicant’s request for a reference that teaches publishing information, Examiner submits US Patent 4,634,807, to Chorley et al. (hereinafter Chorley). Chorley teaches publishing a plaintext message and its corresponding encrypted text (column 3, lines 1-67).”

In the Advisory Action dated May 5, 2006, the Patent Office asserted Chorley teaches publishing the public key, and the particular passage cited provides the teaching that publishing/ knowledge of the encryption key, a plaintext and the corresponding encrypted text does not provide the decryption key.

Chorley discloses (column 3, lines 1-67) “software are operating system independent. The protected module simply forms part of a software package and may be in a language common to all such packages. The unencrypted part of the software is tailored to run on a particular operating system, this part being changed as required for different operating systems. A description of the DES is given in Federal Information

Processing Standard, No. 46, US National Bureau of Standards, 15th Jan. 1977. As mentioned previously, the DES key used to encrypt a message must also be used in decrypting it. **On the other hand, a public-key system is one in which encryption can be carried out using one key, but decryption is carried out using a different key. Knowledge of the encryption key, a plaintext message and its corresponding encrypted text does not, in practice, determine the key used to decrypt the ciphertext, and therefore publishing the encryption key does not significantly decrease the security of its corresponding secret decryption key. ...**

Applicant does not understand how this particular passage discloses or fairly suggests the claim limitation of “the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i .” The most relevant part of the cited passage of Chorley reads “On the other hand, a public-key system is one in which encryption can be carried out using one key, but decryption is carried out using a different key. Knowledge of the encryption key, a plaintext message and its corresponding encrypted text does not, in practice, determine the key used to decrypt the ciphertext, and therefore publishing the encryption key does not significantly decrease the security of its corresponding secret decryption key.” There appears to be no disclosure of “the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i .each test plaintext P_i said corresponding test ciphertext C_i .” **Applicant requests that the Patent Office particularly point out how this passage from Chorley, other passages from Chorley, or other prior art meets this claim limitation.**

Absent such a showing, Applicant believes that claim 7 is allowable for this additional reason.

Issue III

Did the Patent Office properly reject claims 2, 4, 6, 9, and 12 as unpatentable under 35 U.S.C. 103(a) over Kocher et al. and Tschudin as applied to claims 1, 5, 8, and 11 above and further in view of Esserman et al. (US Patent Number 5,144,664)?

Kocher discloses redundancy to determine security compromises through encryption and relates to a smartcard environment. Tschudin discloses checking for a kill signal through decryption and relates to distributed mobile services. Esserman discloses switching encryptors having different security algorithms and relates to broadcasting TV signals. Even if Kocher were combinable with Esserman, one of ordinary skill would not look to Tschudin as Kocher is concerned with encryption and the methodology of Tschudin entails decryption.

Furthermore, none of the references Kocher, Tschudin, or Esserman disclose or suggest the claimed technique which determines the existence of an apoptosis key, considered a compromise situation, when a test plaintext generates a corresponding test ciphertext under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i .

Thus, claims 2, 4, 6, 9, and 12 are not made obvious by Kocher, Tschudin, or Esserman, alone or in combination.

Claim 2

Claim 2 recites “System as claimed in claim 1, wherein said cryptographic system (1) includes at least one second cryptographic algorithm means (8) wherein said switching means (7) enables switching to said at least one second cryptographic algorithm means (8).”

The base reference Kocher uses redundancy to find a defective result and discloses methods for self-checking functions (col. 13, lines 20-55), but does not disclose or fairly suggest a need or desire for switching to a second cryptographic algorithm. Since Kocher concerns minimizing leakage from smartcards and Esserman concerns preventing television signal theft in a subscriber system, one of ordinary skill in the art would not be likely to look to Esserman.

Thus, claim 2 is allowable over the prior art of record. Claim 2 is thus patentably distinct from base claim 1.

Claim 4

Claim 4 recites “System as claimed in claim 1 further comprising a cascaded list of different cryptographic algorithm means.”

Claim 4 is allowable for the reasons provided above and is patentably distinct from base claim 1.

Claim 6

Claim 6 recites “Method as claimed in claim 5, further comprising the step of implementing within said cryptographic system (1) at least one second cryptographic algorithm for said ciphering operations, and switching by said switching means (7) to said at least one second cryptographic algorithm.”

Claim 6 is allowable for the reasons provided above and is patentably distinct from base claim 5.

Claim 9

Claim 9 recites “Method as claimed in claim 8, further comprising the step of switching to one of a plurality of second cryptographic algorithms for said cryptographic operations after said stopping.”

Claim 9 is allowable for the reasons provided above and is patentably distinct from base claim 8.

Claim 12

Claim 12 recites “Computer software product as claimed in claim 11, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to one of a plurality of second cryptographic algorithms for said cryptographic operations after said stopping.”

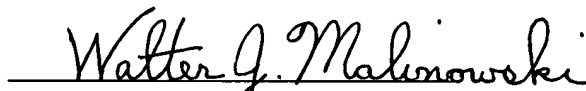
None of Esserman, Kocher, and Tschudin disclose or fairly suggest a control stream includes an apoptosis key and one or more input streams. Thus, claim 12 is allowable over the prior art of record and is patentably distinct from claim 11.

CONCLUSION

For the above reasons, it is respectfully requested that in each of the rejections discussed herein under 35 U.S.C. § 103(a), the Patent Office has failed to meet the burden in establishing a prima facie basis for the rejections of Claims 1-13 and the Patent Office is respectfully requested to reconsider and remove the rejections of the claims under 35 U.S.C. 103(a) of 1, 3, 5, 7, 8, 10, 11, and 13 based on Kocher, U.S. Patent No. 6,327,661, in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services) and the claims 2, 4, 6, 9, and 12 based on Kocher, U.S. Patent No. 6,327,661, in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services) and further in view of Esserman, US Patent Number 5,144,664. Accordingly, reversal of all outstanding rejections is earnestly solicited.

Respectfully submitted,

Dated: August 7, 2006


Walter J. Malinowski
Reg. No. 43,423

Walter J. Malinowski

Harrington & Smith, LLP
4 Research Drive
Shelton, CT 06484-6212
USA
Telephone: 203-925-9400, extension 19
Facsimile: 203-944-0245
Email: wmalinowski@HSpatent.com
www.hspatent.com

(9) CLAIMS APPENDIX

1. A cryptographic system (1) comprising

first cryptographic algorithm means (2) for enabling cryptographic operations, input/output means (3, 4) for receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations,

at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i ,

receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,

checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i ,

switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6).

2. System as claimed in claim 1, wherein said cryptographic system (1) includes at least one second cryptographic algorithm means (8) wherein said switching means (7) enables switching to said at least one second cryptographic algorithm means (8).

3. System as claimed in claim 1, wherein

said receiving means (5) is made for accepting control streams which include at least one plaintext P_i , for each plaintext P_i a corresponding ciphertext C_i and a corresponding apoptosis key K_i and

said checking means (6) is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i .

4. System as claimed in claim 1 further comprising a cascaded list of different cryptographic algorithm means.

5. A method for creating a cryptographic system (1) for carrying out cryptographic operations characterized by the steps of

implementing within said cryptographic system (1) a first cryptographic algorithm enabling said cryptographic operations,

selecting at least one test plaintext P_i and enciphering each test plaintext P_i with said first cryptographic algorithm and with a corresponding apoptosis key K_i thereby generating a corresponding test ciphertext C_i for each test plaintext P_i ,

implementing within said cryptographic system (1) said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i

implementing within said cryptographic system (1) receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,

implementing within said cryptographic system (1) checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i ,

implementing within said cryptographic system (1) switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm, wherein said stopping by said switching means (7) is triggered by said checking means (6).

6. Method as claimed in claim 5, further comprising the step of implementing within said cryptographic system (1) at least one second cryptographic algorithm for said ciphering operations, and switching by said switching means (7) to said at least one second cryptographic algorithm.
7. Method as claimed in claim 5, further comprising the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i .
8. A method for operating a cryptographic system (1) for carrying out cryptographic operations characterized by the steps of
- providing a first cryptographic algorithm for enabling said cryptographic operations, receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations, receiving a control stream which is including at least one apoptosis key K_i , checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i , stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i .
9. Method as claimed in claim 8, further comprising the step of switching to one of a plurality of second cryptographic algorithms for said cryptographic operations after said stopping.
10. Method as claimed in claim 8, wherein said receiving of a control stream includes for each apoptosis key K_i receiving of a plaintext P_i and a corresponding ciphertext C_i , and said checking includes trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , and said received ciphertext C_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i .

11. A computer software product for operating a cryptographic system (1) for carrying out cryptographic operations, said product is characterized by a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, enable the computer to

perform a first cryptographic algorithm that is enabling said cryptographic operations,

receive input streams and send output streams wherein said input streams are transformed to said output streams by said cryptographic operations,

receive a control stream which is including at least one apoptosis key K_i ,

check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i ,

stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i .

12. Computer software product as claimed in claim 11, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to one of a plurality of second cryptographic algorithms for said cryptographic operations after said stopping.

13. Computer program comprising program code means for performing the steps of claim 8 when said program is run on a computer.

(10) EVIDENCE APPENDIX

Applicant proffers no evidence.

(11) RELATED PROCEEDINGS APPENDIX

The undersigned attorney is not aware of any related appeals or interferences.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail on the date shown below in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

8/7/2006
Date

Elaine F. Mian
Elaine F. Mian